Method for generating and verifying digital watermarks and for exchanging data containing digital watermarks

Cross References to Related Applications

This application claims the priority of European patent application 97810708.4, filed Sept. 26, 1997, the disclosure of which is incorporated herein by reference in its entirety.

Technical Field

The present invention relates to methods for generating and verifying digital watermarks and for transmitting data containing digital watermarks according to the preamble of the independent claims.

Background Art

Digital watermarking is a method for marking data sets, such as images, sound or video. A digital watermark consists of a slight modification of the data set that does not affect the data set's usability but that can be detected using dedicated analysis software or apparatus. Watermarking can e.g. be used for marking authorship or ownership of a data set. It can also be applied for verifying the originality of the multimedia data content, where the loss of originality refers to the degree of contents modification suffered by the image.

Digital watermarking can be seen as a fundamental-problem in digital communications (see e.g. I. Cox, J. Killian, T. Leighton, and T. Shamoon, "Secure spread spectrum communication for multimedia", Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996). Early methods of encoding watermarks consisted of no more than increment-

ing an image component to encode a binary '1' and decrementing to encode a '0' (G. Caronni "Assuring Ownership Rights for Digital Images" in H. H. Brueggemann and W. Gerhardt-Haeckl, editors, Reliable IT Systems VIS '95, Vieweg Publishing Company, Germany, 1995). Tirkel et al. (A. Z. Tirkel, G. A. Rankin, R. G. van Schyndel, W. J. Ho, N. R. A. Mee, and C. F. Osborne, "Electronic watermark", in Dicta-93, pages 666-672, Macquarie University, Sydney, December 1993) and van Schyndel et al. (A. Z. Tirkel, R. G. van Schyndel, and C. F. Osborne, "a two-dimensional digital watermark", in ACCV'95, pages 378-383, University of Queensland, Brisbane, December 6-8 1995) have applied the properties of m-sequences to produce oblivious watermarks resistant to filtering, cropping and reasonably robust to cryptographic attack. Matsui and Tanaka (K. Matsui and K. Tanaka, "Video-Steganography : How to secretly embed a signature in a picture", in IMA Intellectual Property Project Proceedings, pages 187-206, January 1994) have applied linear predictive coding for watermarking. Their approach to hiding a watermark is to make the watermark resemble quantization noise. Tirkel and Osborne (see above) were the first to note the applicability of spread spectrum techniques to digital image watermarking. Since then there has been an increasing use of spread spectrum in digital watermarking. It has several advantageous features, such as cryptographic security (see Tirkel and Osborne, above), and is capable of achieving error free transmission of the watermark near or at the limits given by the maximum channel capacity (J. Smith and B. Comiskey, "Modulation and information hiding in images", in Ross Anderson, editor, Proceedings of the First International Workshop in Information Hiding, Lecture Notes in Computer Science, pages 207-226, Cambridge, UK, May/June 1996. Springer). Fundamental information theoretic limits to reliable communication have been discussed by some authors (see Smith and Comiskey, above). The shorter the

payload of a watermark, the better are the chances of it being communicated reliably. Spread spectrum is an example of a symmetric key cryptosystem (B. Schneier, "Applied Cryptography", Wiley, 2nd edition, 1995). System security is based on proprietary knowledge of the keys (or pseudo random seeds) which are required to embed, extract or remove an image watermark. One provision in the use of a spread spectrum system is that it is important that the watermarking be non-invertible because only in this way can true ownership of the copyright material be resolved (S. Craver, N. Memon, B. Yeo, and M. Yeung, "Can invisible marks resolve rightful ownership's ?", IS&T/SPIE Electronic Imaging '97 : "Storage and Retrieval of Image and Video Databases", 1997). Ó Ruanaidh et al. (J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Phase watermarking of images", IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996) and Cox et al. (see above) have developed perceptually adaptive transform domain methods for watermarking. In contrast to previous approaches listed above the emphasis was on embedding the watermark in the most significant components of an image or a video frame. The general approach used in these papers is to divide the image into blocks. Each block is mapped into the transform domain using either the Discrete Cosine Transform (W. B. Pennebaker and J. L. Mitchell, "JPEG Still Image Compression Standard", Van Nostrand Reinhold, New York, 1993), the Hadamard Transform (W. G. Chambers, "Basics of Communications and Coding", Oxford Science Publications. Clarendon Press Oxford, 1985) or the Daubechies Wavelet Transform (W.H. Press, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery, "Numerical Recipes in C", Cambridge University Press, second edition, 1992). The phase component of the image or video frame is then modified according to the pseudo-random sequence containing the watermarking information.

Information can be embedded using the DCT (J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, "Watermarking digital images for copyright protection", IEEE Proceedings on Vision, Image and Signal Processing, 143(4) :250-256, August 1996, based on the paper of the same title at the IEEE Conference on Image Processing and Its Applications, Edinburgh, July 1995) FFT magnitude, and phase, Wavelets (see refs. of Ruanaidh, Dowling and Boland, above), Linear Predictive Coding (see Matsui et al., above) and fractals (P. Davern and M. Scott, "Fractal based image steganography", in Ross Anderson, ed., Proceedings of the First International Workshop in Information Hiding, Lecture Notes in Computer Science, pp. 279-294, Cambridge, UK, May/June 1996. Springer Verlag).

The key to making watermarks robust has been the recognition that in order for a watermark to be robust it must be embedded in the perceptually significant components of the image (see ref. of Ruanaidh, Dowling and Boland, and ref. of I. Cox, J. Killian, T. Leighton, and T. Shamoon above). Objective criteria for measuring the degree to which an image component is significant in watermarking have gradually evolved from being based purely on energy content (see refs. of Ruanaidh et al., Cox et al. above), to statistical (see I. Pitas, "A method for signature casting on digital images", Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996) and psychovisual (see J.F. Delaigle, C. De Vleeschouwer, B. Macq, "Digital watermarking", Proceedings of the SPIE Electronic Imaging: Science and Technology, vol. 2659: Optical Security and counterfeit Deterrence Techniques, San Jose, February 1996 and M.D. Swanson, B. Zhu and A. Tewfik, "Transparent robust image watermarking", Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, September 1996).

The industrial importance of digital watermarking has resulted in a number of products on the mar-

ket, either based on spread spectrum techniques or additional registration services. They include the Picturemarc system by Digimarc (RHOADS, B. Geoffrey, Digimarc Corp (US), "Steganography Systems, WO 96/36163 A, SureSign (former FBI's Fingerprint) by HighWater Signum (WO 96/27259), IP_2 system by Intellectual Protocols, the Argent system by Digital Information Commodities Exchange, the PixelTag system by the MIT Media Lab, the SysCop system from Zhao and Koch by the Frauenhofer-Institut für Graphische Datenverarbeitung (J. Zhao and E. Koch, "Embedding robust labels into images for copyright protection", Proceedings of the International Congress on Intellectual Property Rights For Specialized Information, Knowledge and New Technology, August 1995 J. Zhao, "A WWW Service To Embed And Prove Digital Copyright Watermarks", Proc. Of the European Conference on Multimedia Application, Services and Techniques, vol. 2, Louvain-La-Neuve, Belgium, May 1996), and the Tigermark system from NEC (European patent Application EP 766468A, Nippon Electric Corporation (NEC), April 1997)

The approach proposed by Digimarc (see WO 96/36163) adds or subtracts small random quantities from each pixel according to the least significant bit of each pixel compared with the binary mask. The originality of their approach consists in the use of "subliminal digital graticules" that will help in recovering a rotation R and a scaling S performed on the marked image. They use an exhaustive search strategy based on these graticules to recover R and S. This stands in contrast to the template embodiment described here, where the use of log-polar or log-log mapping of the Fourier transform of the image combined with cross-correlation in the log-polar or log-log plane avoid such a search.

The Highwater approach (WO 96/27259) describe a permutation technique to modify the values of the data elements according to certain rules which depend on the message.

The approach of Zhao and Koch, based on the JPEG image compression algorithm, proceeds by segmenting the image into individual 8 x 8 blocks. Only eight coefficients occupying particular positions in the 8 x 8 block of DCT coefficients can be marked. These comprise the low frequency components of the image block but exclude the mean value coefficient as well as the low frequencies. Three of the remaining DCT coefficients are selected using a pseudo random number generator to convey information. The resemblance of this technique to frequency hop spread spectrum communications is also mentioned and the blocks are placed at random positions in the image. A WWW registration service has been proposed for a local registration and a local watermarking, for a server registration and a server watermarking, and for a local watermarking and a server registration. The approach is based on a trusted third party model (WWW server and Watermark Embedding Gateway). This model requires from the Copyright Holder the transfer of relevant confidential information applied for the watermarking process. It is, therefore, possible that the owner of the trusted third party system may impersonate the Copyright Holder and infringe his copyright. Since the applied key for the embedding is not a cryptographic key, copyright protection and communication security are addressed by two different technical solutions, namely the SysCop system and the s-http protocol. These two technical solutions are applied independently. There is no third party verification procedure supported which allows the verification of the seed, applied for the embedding of the watermark, by independent parties, such as a court of law. The s-http protocol (SSL security protocol) differs from the protocol presented below in many aspects (for example, the non-repudiation security service is not supported by the s-http protocol). The keys applied for the embedding of the mark are furthermore not registered in the SysCop system. For copyright verification, the Copy-

right Holder has to disclose his key. The information generated by the trusted third party is based on the cover data, but not on the stego data.

I. Cox et al from NEC (see EP 766 468, above) propose to insert watermark into the perceptually significant components of a decomposition of the data in a manner so as to be visually imperceptible. In contrast to the method described here, they need the original data which is compared to the watermarked data to obtain an extracted watermark.

J.-F. Delaigle at al. (J.-F. Delaigle, J.-M. Boucqueau, J.-J. Quisquater and B. Macq, "Digital Images protection techniques in a broadcast framework: An overview", Proceedings of the European Conference on Multimedia applications, Services and Techniques, vol. 2, Louvain-La-Neuve, Belgium, May 1996, J.-F. Delaigle, C. De Vleeschouwer & B. Macq,"Digital Watermarking", Proceedings of the SPIE, vol. 2659, 1 February 1996) have applied signature labeling techniques for the copyright protection of digital images. The approach presented is very similar a EDI security standards. The labeling does not influence the multimedia data. Their approach is based on an enhanced image format and generates a digital signature label in front of the image. This signature label can be easily overwritten or destroyed. The registration entity supports no secure on-line communication protocol and is constrained by a legal trusted third party. In addition, no means are provided to resolve a conflict if multiple watermarks have been embedded in the same image. In an enhanced architecture they propose a general watermarking function which uses the output of a hash function as the payload of the watermark. This watermark function does not support third party verification and is not based on a spread spectrum technique. In addition, different types of watermarks are not supported. The masking scheme presented depend on a ciphering function for the inscription. In contrast to the approach pre-

sented in this disclosure, the secret key has to be revealed for copyright verification and no coding/decoding along with cryptographic digital signatures are applied. In addition, the cryptographic key applied is only used for ciphering and not for other functional purposes relevant for copyright protection as defined in this disclosure.

S. Matyas at all (Stephen M. Matyas, Donald B. Johnson, An V. Lee, Rostislaw Prymak, William C. Martin, William S. Rohland, and John D. Wilkins, "EP 0 534 419 A", Stephen M. Matyas, Donald B. Johnson, An V. Lee, Rostislaw Prymak, William C. Martin, William S. Rohland, and John D. Wilkins,"EP 0 539 726 A") have specified a system which is based on an architecture with two different entities, namely the data processor with a cryptographic system and the network certification center. The overall system security depends on a hierarchical cryptographic key scheme and digital certificates are only generated for a specific data set, called control vectors. These control vectors set up the basis to identify the access rights of users and associated processes they have initiated. The main focus of the specified system is the enforcement of a dedicated security policy which is based on a hierarchical role model. The system is based on a hardware based security processors and applies symmetric and asymmetric cryptographic keys. The cryptographic protocols applied are different to the protocols presented in this disclosure. The emphasis is to provide a method for controlling the use of private and public keys which is not the purpose of our system. In addition, one entity needs several different types of keys (symmetric and asymmetric) in contrast to our approach which uses for one entity one asymmetric key pair only.

Tanaka et al. (K. Tanaka and K. Matsui, "A Digital Signature scheme on a Document for MH Facsimile Transmission", Electronics & Communications in Japan, Part I - Communications, Vol. 74, No. 8, August 1991)

propose a digital signature scheme for watermarking facsimile documents (binary images). This scheme modify the length of certain runs of data with a single bit of the signature data.

Disclosure of the Invention

It is an object of the present invention to provide a system of the type mentioned above that provides a simple and secure way of generating and transmitting watermarked data. This object is achieved by the methods described in the claims.

In one aspect of the invention, this object is achieved by an integrated solution method for generating and transmitting a data set between two parties H and B comprising the steps of a) providing a cover data set corresponding to the data set to be transmitted, b) generating a stego data set of said cover data set by embedding at least one digital watermark in said cover data set, wherein said watermark is encoded using at least one key of an asymmetric cryptographic key pair of H, said key pair comprising a secret private key and a known public key derived therefrom, and c) encrypting said stego data set using said key pair of H, d) transmitting said encrypted stego data set from said party H to said party B.

The party creating the watermark can embed a detection, a private and a public watermark in the data set, wherein the detection or the private watermark is derived from the private key, the public watermark from the public key. The public watermark can be detected by third parties while the private watermark can only be detected using private information. Preferably, the detection or private watermark is not derived from the private key directly but from a hash value of the same and/or from a signature generated with the same, such that the

author of the watermark does not have to reveal his private key if the private watermark is to be verified.

In another aspect of the invention, the cover data set is provided with a digital watermark and derived stego data then securely transmitted to a registration party that permanently stores at least time information, origin of the stego data set, and a digital copyright certificate.

In another aspect of the invention, a template modulation pattern is added to the Fourier transform of an image that is to be provided with a watermark. For checking the watermark, the Fourier transform of the stego-image is calculated. From this Fourier transform, the log-polar mapping transform is generated, which is then searched for the modulation pattern. Using the log-polar transform of the Fourier transform has the advantage that scaling and rotation of the stego-image are expressed in translations. This allows an easy search for rotation and scaling using cross-correlation techniques.

However, especially for video data, a change of proportion (different horizontal and vertical scaling) is more probable than a rotation. In such cases, the template modulation pattern is rather searched in the log-log transform of the Fourier transform. Similarly to the log-polar map, the log-log map allows to express the horizontal scaling and vertical scaling in translations and cross-correlation techniques can be applied to search the template.

In still another aspect of the invention, the image to be watermarked is divided into blocks and the magnitude components of the Fourier transform of each block is modulated using the same pattern. This method provides robustness against cropping of the stego-image because a cropping leads to a circular translation in each block. Preferably, the magnitude components of the Fourier transform are modulated, wherein the sign of the modulation should be derived from the phase components,

thereby reducing interference between the image data and the watermark as explained in the following disclosure.

In a further aspect, the invention consists of a method for generating and transmitting a data set between two parties H and B comprising the steps of providing a cover data set corresponding to the data set to be transmitted, generating a stego data set of said cover data set at a party H by generating at least one digital watermark in said cover data set, transmitting a has value of said stego data set to a registration party, and permanently storing certification data at said registration party, said certification data comprising said hash value of said stego data set, a digital time stamp and information designating said party H.

In a further aspect, the invention relates to a method for generating a stego data set from a cover data set by adding a watermark to said cover data set comprising the steps of dividing said stego data sets into blocks, calculating a lapped orthogonal transform of each of said blocks, and applying said watermark to said lapped orthogonal transforms.

In another aspect, the invention relates to a method for generating a watermark in a cover data set (CD) representing a two or three dimensional data set, especially for step b) of one of the preceding claims, comprising the following steps: A) generating a template modulation pattern (**T'**) using a random number generator seeded by a key (K), B) calculating the Fourier transform of at least part of said cover data set (CD) for generating Fourier components of said cover data set, C) modulating at least part of said Fourier components using said template modulation pattern (**T'**), D) using the inverse Fourier transform for generating a stego-image

The invention further relates to a method for verifying a watermark in a possibly rotated and/or scaled version of a two or three dimensional stego data set, comprising the steps of: A) calculating a Fourier trans-

form of said stego data set (SD), B) calculating a log-polar or a log-log transform of said Fourier transform of said stego data set, and C) calculating the correlation between said log-polar or log-log transform and a template (**T**), which template is the log-polar or log-log transformation of said watermark.

Brief Description of the Drawings

The invention will be better understood and objects other than those set forth above will become apparent when consideration is given to the following detailed description thereof. Such description makes reference to the annexed drawings, wherein:

Fig. 1 the parties involved in individual watermark protection,

Fig. 2 the parties involved in watermark protection using registered cryptographic keys,

Fig. 3 the parties involved in watermark protection using registered cryptographic keys and a registration party,

Fig. 4 the steps taken for embedding a watermark,

Fig. 5 the steps for generating the template,

Fig. 6 the steps for reading a watermark,

Fig. 7 the steps for reading the template,

Fig. 8 the steps for embedding watermark in a rotation, scale and translation invariant domain,

Fig. 9. the steps for embedding the watermark in an image avoiding to map the original image into the rotation, scale and translation invariant domain,

Fig. 10. the steps to extract the watermark from the image,

Fig. 11 the tiling of the watermark in a stego-image or stego video frame, and

Fig. 12 the tiling of the watermark in a cropped stego-image or cropped stego video frame.

Modes for Carrying Out the Invention

I. Terms and Symbols:

Before describing a preferred method and apparatus according to the invention, some key terms and symbols used in its description are explained in the following:

"Image": An image in either digital or physical form which may constitute a still image or a video frame. It can also refer other types of data, such as video and sound, in particular when being used within the context of the protection and owner authentication methods of section II of the disclosure.

"Signal": A signal in either digital or physical form. It may refer to one dimensional or multi-dimensional signals such as image and video.

"Copyright Holder (CH)": A party (or a process acting on behalf of it) "owning" a digital image or video. This is the party that generates the watermarks.

"Buyer (B)": A party (or a process acting on behalf it) which obtains (e.g. by purchase) via electronic means a specific image from the CH.

"Stego": Implies that an image or video data is marked. The stego image is also referred to as the stego data set (e.g. stego image or video frame).

"Cover": Implies that an image or data is unmarked. The cover image is also referred to as the cover data set (e.g. cover image or video frame).

"Watermark": The form the IAD takes when it is in a form suitable for embedding in a signal.

"Copyright Certificate Center (CCC)": An organization (or a process which acts on behalf of it) which registers copyright ownership for a specific image

or video. Successful registration is only based on a sender verification procedure. After successful registration a digital copyright certificate can be generated. The CCC does not act as trusted third party in our system.

"Digital copyright certificate": Digital copyright data which comprise the copyright certificate data and a digital signature.

"Copyright Request Data (CRD)": Copyright data which contains the stego-image, the image ID of the cover-image, a Universal Copyright Convention Notice, a Copyright Symbol, the term ''Copyright'', the year of the copyright, the name of the copyright holder, and the phrase ''All Rights Reserved''.

"Copyright Certificate Data (CCD)": Copyright data which contains relevant copyright information.

"Digital signature": A data string which has been generated by a cryptographic digital signature generation transformation.

"Digital signature generation transformation": A method for producing a digital signature.

"Digital signature verification transformation": A method for verifying whether a digital signature is authentic or not.

"Digital signature scheme": A scheme based on asymmetric cryptographic techniques whose private transformation is used for the digital signature generation and whose public transformation is used for the digital signature verification.

"Digital signature scheme with message recovery": A digital signature scheme for which a priori knowledge of the input data is not required for the signature verification transformation.

"Digital signature scheme with appendix": A digital signature scheme for which the input data is required as input to the digital signature verification transformation.

"Asymmetric key pair": A pair of related cryptographic keys where the private key defines the private transformation and the public key defines the public transformation.

"Symmetric key": A cryptographic key used with a symmetric cryptographic technique and known only to a set of specified entities.

"Public Key Infrastructure (PKI)": An organization (or processes which acts on behalf of it) which offers services for the generation, registration, certification, distribution, validation, and revocation of a certificate associated with an asymmetric key pair.

"Public watermark": A watermark that can be detected using a publicly available key (or a hash value thereof).

"Private watermark": A watermark that can only be detected using a secret key (or a hash value thereof) and some data associated to specific cover data. It is not possible for an unauthorized third party to overwrite or delete the private watermark without the cryptographic secret keying information.

"Detection watermark": A watermark that can only be detected using a secret key (or a hash value thereof). It is not possible for an unauthorized third party to overwrite or delete the private watermark without the cryptographic secret keying information.

"Payload": The core of the hidden IAD in bit form without error control coding applied.

"Image ID": The following format scheme for a globally unique ID: The first 3 bytes determine the CCC, the following 3 bytes determine the CH ID defined by the CCC. Finally the CH can freely assign last 4 bytes for each one of his digital images or videos.

"Oblivious": A watermarking technique which does not require the cover-image for extracting the mark. In other words, only the stego-image is required to extract the mark when using an oblivious marking scheme.

"Template": A hidden message encoded in the image. Two kind of templates are used: "RST template (Rotation-Scale Template) " and "PST template" (Proportion-Scale Template). By detecting the RST template, the scaling (zooming) and rotation suffered by a stego-image can be determined. By detecting the PST template, the horizontal and the vertical scaling are detected, and therefore the change of proportion suffered by a stego-image can be determined.

"Pseudo random seed": A value used to initialize a pseudo random number generator.

"Modulation": Changing a component's value e.g. by addition or multiplication.

Symbols:

H, C, B, I
: Distinguished (unique) name of the Copyright Holder, the Copyright Certificate Center, the Buyer B and the Public Key Infrastructure I.

Cert H , Cert C, Cert B
: Entity H's public key certificate from I, entity C's public key certificate from I and entity B's public key certificate from I.

(ps_X , vs_X)
: The asymmetric signature and verification key pair of an entity with the distinguished name X.

(pc_X , vc_X)
: The asymmetric decipherment and encipherment key pair of an entity with the distinguished name X.

CC
: A copyright certificate

$DSSMR_G (X,Y,Z)$
: A digital signature generation scheme with message recovery, where X denotes the private key, Y the input data, and Z the resulting signature.

$DSSMR_V(X,Y,Z)$

A signature verification scheme with message recovery, where X denotes the public key, Y the input data, and Z the resulting output data.

$DSSAP_G(X,Y,Z)$

A digital signature generation scheme with appendix, where X denotes the private key, Y the input data, and Z the resulting signature.

$DSSAP_V(X,Y,Z)$

A signature verification scheme with appendix, where X denotes the public key, Y the input data, and Z the resulting output data.

crh A collision resistant hash function

OWEA(X,Y,CD, SD)

The oblivious, spread spectrum based watermark embedding algorithm with the seed X, the payload Y, the cover data CD, and the resulting stego data SD.

OWVA(X,SD,Y)

The oblivious, spread spectrum based watermark verification algorithm with the seed X, the stego data SD, and the resulting payload Y).

TVP

Time variant parameter, such as a sequence number or a time stamp.

RPMG(X,Y)

A random phase mask generator, where X denotes the cryptographic key as input data and Y denotes the resulting phase mask as output data.

DIES(PM,OI,CD)

A symmetric digital image encryption scheme, which is based on the Fourier transform of the image, phase modification (random mask encoding by multiplication on the complex exponential component $e^{j\varphi(m,n)}$), inverse Fourier transform, and quantization, where PM denotes the phase mask and ID denotes the original image as input data and OI denotes the ciphered image as output data.

FFTS(CO, S_R, SMC)

A component selector function of the real and imaginary FFT components. CO denotes the cover image, S_R the applied selection rule function, and SMC the resulting set of FFT magnitude components.

AF(SMC, HF, MS)

An authentication function of the selected FFT magnitude components, where SMC denotes the identified magnitude components, HF denotes the applied crh, and MS the resulting authentication message as a string of arbitrary length. For example, AF(SMC, HF, MS) consists of generating a string from each selected Fourier component, concatenating these strings and applying a hash function to the resulting string.

K_{XY}

A secret key for a symmetric cryptosystem shared between two entities with the distinguished name X and Y.

K_{XY}[Data]

denotes the cipher text generated by a symmetric cryptosystem with plain text Data.

||

Concatenation of two data elements.

CD

Cover Data

SD

Stego Data

II. Copyright/Content/Originality protection based on a spread spectrum technique

Depending on the proof-level to be provided for the protection, the preferred embodiment of the apparatus and method according to the invention provides three different levels of reliability, which are based on each other, namely: individual copyright/content/origin-

ality protection, copyright/content/originality protection with registered cryptographic keys, and copyright/content/originality protection with an CCC on the basis of registered cryptographic keys.

Due to commercial requirements, the system provides different protection aspects, nameley content protection, copyright protection, and originality verification of the stego data.

The copyright protection of a multimedia data set is considered as the process of proving the intellectual property rights to a court of law against unauthorized reproduction, processing, transformation, or broadcasting on the basis of digital evidence data. This process is based on a watermarking process WP and a registration process RP. RP is executed after WP has been initiated and finished. RP is executed by a third party, which represents a different legal entity as the Copyright Holder (CH), and provides digital evidence data for the CH required for verifying copyright ownership. The specific cover- or stego data is a digital image, or video data. The WP embeds or extracts owner authentication data in or from multimedia data sets. This owner authentication data is embedded such that the commercial usability of the multimedia data set is not affected. For this purpose, a key is applied to embed encoded owner authentication data, called the watermark, into the cover data set I, resulting in a stego data set I*. The watermark data can then be extracted from the stego data if the correct key is used.

In the following, WP is based on a perceptually adaptive spread spectrum technique, a specific type of a symmetric cryptographic system. In order to embed or extract a watermark, it is necessary to know the exact values of the seed used for the generation of pseudo random sequences used to encode the watermark. Because spread spectrum signals are statistically independent (and therefore virtually orthogonal), more than one wa-

termark may be encoded into the multimedia data set. Depending on the seed applied for the embedding and verification, we distinguish between a private and a detection watermark. A private watermark is defined as encoded owner authentication data embedded with a cryptographic signature as the seed. A detection watermark is defined as encoded owner authentication data embedded with a cryptographic secret key as the seed. We differentiate between copyright protection, content protection, and originality protection.

Originality protection is considered as a process applied after the copyright protection process. It enables a third party to check if the image contents has been modified on the basis of a public watermark.

Content protection is considered as an additional process applied during the trading transaction between a service provider and a customer. The content protection described is based on the transform domain of the image data and not on cryptographic ciphering algorithms applied during the communication between the service provider and the customer, since these cryptographic algorithms are not robust against loosely compression and other image transformations. In addition, the performance of ciphering algorithms for the content protection of image or video data is very time consuming.

The present method and apparatus is based on an image or video watermark technique, described below, which embeds and detects the the payload of a watermark. This technique is based on a perceptually adaptive spread spectrum technique which provides reliable means of embedding robust watermarks. Such a technique will be discussed in section III. In addition, a spread spectrum techniques is a form of symmetric cryptosystem. In order to embed or extract a watermark, it is necessary to know the exact values of the seed used to produce pseudo random sequences used to encode a watermark. The seeds are

considered to be cryptographic keys for watermark generation and verification. System security can therefore be based on proprietary knowledge of the keys and provide in addition the necessary security parameters needed for a secure communication (mutual authentication, integrity, confidentiality, non-repudiation) in the trading process of digital images or videos. Because spread spectrum signals are statistically independent (and therefore virtually orthogonal), the present method and apparatus encodes more than one watermark in an image or video frame at the same time, namely detection, private watermarks and public watermarks. The detection watermark allows to identify during a scanning process if the stego data belongs to the copyright material of a CH. The generation of the private watermark is based on a digital signature as the seed and supports, therefore, third party verification who has generated the seed information for the coding and the decoding of the payload. The generation of the public watermarks enable the verification of the originality of the received stego data. on the private key of the asymmetric key pair of the ICH.

Since the system provides for the registration of the public key of the asymmetric key pair, the CH can prove that he is the only person in the possession of the adequate private key of the asymmetric key pair and, therefore, the generator of the private watermarks.

The system also provides the secure registration (mutual authentication, integrity, non-repudiation) of watermark encoded images (stego data sets) at a CCC. The stego-image is registered at the CCC and a digital copyright certificate is generated which is signed by the CCC. If an unauthorized third party has also encoded watermarks in the same image, conflicting claims in copyright disputes can be resolved. Examining the time stamps of the copyright certificate enables the secure identification of the legal owner: The earliest of the time

stamps identifies the legal owner if no copyright revocation request has been applied.

Watermark protection with registered cryptographic keys and the CCC based copyright protection are based on a PKI. The PKI issues on request public key certificates containing the public key of the party, the distinguished name of the party, and a time stamp. Every certificate is signed with the PKI's private key and the trust is built on the validity of the authentic copy of the PKI's public key (we assume that the public key of the PKI is accessible, authentically distributed, and verifiable by every party).

In the following three levels of the system are described.

The method described in this section II requires a suitable watermarking technique. Various such techniques are known and can be employed. However, a preferred technique is described in the section III.

II.a) Registration based copyright, content, and originality protection

Depending on the proof-level to be provided for the protection, our approach provides three different protection levels, which are based on each other, namely individual copyright/content/originality protection, copyright/content/originality protection with registered cryptographic keys, and copyright/content/originality protection with a CCC on the basis of registered cryptographic keys. Since the first two cases are special cases of the third one, we present only the approach for the registration based copyright protection. Depending on the level of protection to be provided (content or originality or copyright protection), not all phases described below have to be executed. The phases described below have to be executed for the highest level of protection, i.e. content and originality and copyright protection. Based on one asymmetric key pair only, H can enforce the

different protection mechanisms for copyright, originality, and content protection.

As shown in Fig. 3, the system for the CCC based protection is partitioned into four processes, namely the CH with the name H, the B process with the name B, the PKI process with the name I, and the CCC process with the name C. Suppose (ps_H, vs_H), (pc_H, vc_H), (ps_B, vs_B), (pc_B, vc_B), (ps_I, vs_I), (pc_I, vc_I), (ps_C, vs_C), and (pc_C, vc_C) are the asymmetric key pairs of H, B, I and C, respectively and all the involved parties would like to exchange information by on-line communication. (In the case of off-line communication, the security mechanisms to be provided for the communication are covered by operational means). H has an authentic copy of $Cert_B$ and $Cert_C$ whose signatures were verified with the authentic copy of vs_I . B has an authentic copy of $Cert_H$ and $Cert_C$ whose signatures were verified with the authentic copy of vs_I. C has an authentic copy of $Cert_H$ and $Cert_B$ whose signatures were verified with the authentic copy of vs_I. The following phases are then applied:

Phase 1:
H retrieves the cover data CD, generates a unique identifier $ID_{CD} := crh(H||SN)$, where SN is a serial number, stores ID_{CD}, and retrieves the key pair (ps_H, vs_H).

Phase 2:
Detection watermark embedding (image owner authentication and copyright protection)
H generates the stego data SD applying the transformation: $OWEA(crh(ps_H), SN||SN, CD, SD)$.

Phase 3:
Private watermark embedding (copyright protection)

1. H generates the private Owner Authentication Data OAD_{CD} applying $DSSMR_G(ps_H, ID_{CD}, OAD_{CD})$.
2. H generates the stego data SD applying the transformation: $OWEA(crh(OAD_{CD}), ID_{CD}, CD, SD)$, where CD is the SD of the last phase.

Phase 4:

Public watermark embedding (originality protection)

1. H generates the set of magnitude components, applying FFTS(CD, S, MC), with the selection function S and the resulting set MC of the FFT magnitude components. S is given by the normalization of the magnitude components with the JPEG or MPEG quantization table entries and constrained by these components that will be modified during the coding process of the public watermark.
2. H then generates the authentication data for originality verification, applying AF(MC, crh, AM), where MC denotes the in the last step generated FFT magnitude component set, crh the applied hashing function, and AM the resulting authentication message as output. AM is generated by converting the value of every magnitude component into a string and concatenating the resulting strings of every magnitude component into one string.
3. AM is then ciphered with the key pc_H, i.e. pc_H[AM] and embedded as the payload in the public watermark, applying OWEA(crh(vs_H),pc_H[AM],CD, SD), where CD is the SD of the last phase.

Phase 5:

H then stores the resulting stego data SD.

Phase 6:

H and C execute the following steps for the secure registration or validation of copyright requests, and the generation of copyright certificates.

1. H generates first the copyright request data CRD, CRD := crh(SD||SN) and then the copyright request CR, CR := <TD||SigTD>, with TD := CRD|| TVP||H||C, and $DSSAP_G(ps_H$, TD, SigTD). H then transmits CR to C.
2. C receives CR and verifies TD, applying $DSSAP_V$ (vs_H, SigTD, IVR), where IVR denotes the intermediate verification result. If IVR = crh(TD), with TD := CRD||TVP||H||C, then TD has been successfully veri-

fied and the next step shall be executed. In any other case, the processing and communication between the H and C is stopped.

3. If verification was successful, C generates the corresponding digital copyright certificate executing $DSSAP_G(ps_C, CCD, SigCCD)$, with CCD:= CRD||TVP. C then stores the copyright certificate CC := CCD||SigCC and generates then the Copyright Confirmation Reply CCR, CCR := <TD||SigTD>, with TD := CC||TVP||C||H, and $DSSAP_G(ps_C, TD, SigTD)$. C then transmits CCR to H.

4. H receives CCR and verifies TD, applying $DSSAP_V(vs_H, SigTD, IVR)$, where IVR denotes the intermediate verification result. If IVR = crh(TD), with TD := CC||TVP||C||H, then TD has been successfully verified. H then verifies and stores the CC. The following phase can now be executed repeatedly, if necessary, without repetition of the previous phases.

Phase 7:

H and B execute the following steps for the trading of copyright, content, and originality protected digital data (images and video):

1. B generates the trading transaction T1, T1 := <TD||SigTD>, with TD := ID_{CD}||TVP||B||H, and $DSSAP_G(ps_B, TD, SigTD)$. B then transmits T1 to H.

2. H receives T1, verifies TD, applying $DSSAP_V(vs_B, SigTD, IVR)$ where IVR denotes the intermediate verification result. If IVR = crh(TD), with D := ID_{CD}||TVP||B||H, then TD has been successfully verified and the next step shall be executed. In any other case, the processing and communication between the H and B is stopped.

3. If the verification was successful, H retrieves with the ID_{CD} information the corresponding stego data SD and generates the trading transaction T2 := <TD||SigTD>, with TD := CD||TVP||H||B, DIES(PM, SD, CD) with $RPMG(DSSMR_G(ps_H, B||SN), PM)$, and $DSSAP_G(ps_H,$

TD. SigTD). B||SN designates the B and the picture and is called the mask message. H then stores $DSSMR_C(ps_H, B||SN)$ and transmits T2 to B.

Phase 8:

B receives T2 and verifies TD, applying $DSSAP_V(vs_H, SigTD, IVR)$, where IVR denotes the intermediate verification result. If IVR = crh(TD), with TD := CD||TVP||H||B, then TD has been successfully verified and CD is locally stored.

Phase 9:

After B has paid, H retrieves IK_B and sends $vc_B[IK_B]$. B receives $vc_B[IK_B]$, deciphers it ($pc_B[vc_B[IK_B]]$), and generates the random phase mask PM. This random phase mask is then used for deciphering CD (DIES(PM, CD, SD))to get the original stego data SD.

Phase 10:

B may verify the originality of the stego data SD, retrieving the public key from H and applying $OWVA(crh(vs_H), SD, pc_H[AM])$. B then deciphers $pc_H[AM]$ applying $vc_H[pc_H[AM]]$. H then verifies AM applying the same steps 1 and 2 as described in phase 4. If the verification was successful, the image content has not been altered. If the watermark has been destroyed or overwritten, the contents of the SD has been modified. If the verification fails, the content has also been modified by unauthorized parties.

Remark:

Depending on the applied asymmetric scheme the private decipherment key may be identical to the private signature key and the public encipherment key may be identical with the public verification key.

Since the generated asymmetric key pairs are unique, the CH can be uniquely identified on the basis of the digital copyright certificate.

B may check the copyright certificate requesting C (or H) to transfer an authentic copy of the copyright certificate for a given identifier ID_{CD}. Except

the data transferred, the applied protocol is the same as described above (see phase 6).

If H would like to transfer a specific copyright of a CD set to another legal party, he may initiate a copyright revocation request with C. The different phases of this request are analogue to the copyright request.

For copyright verification, the CH first verifies the detection watermark and then the private watermark with the extracted SN.

Copyright verification may be checked by a third party, if the H transfers the digital signature applied for the seed. Based on the retrived bublic key from H, the third party can verify that H is the only one who has generated the corresponding signature.

II.b) Copyright, content, and originality protection with registered keys

As shown in Fig. 2, the apparatus for the copyright, content, and originality protection with registered cryptographic keys is partitioned into three processes, namely the CH with the name H, the Buyer process with the name B, and the PKI process with the name I. Suppose (ps_H, vs_H), (pc_H, vc_H), (ps_B, vs_B), (pc_B, vc_B), (ps_I, vs_I), and (pc_I, vc_I) are asymmetric key pairs of H, B, and I, respectively. Suppose H has an authentic and actual copy of $Cert_B$ which signature was verified with the authentic copy of vs_I and the B has an authentic and actual copy of $Cert_H$ which signature was verified with the authentic copy of vs_I. Then the same phases except phase 6 as for II.a) have to be applied.

Remark:

Since the generated asymmetric key pairs are unique, the CH can be uniquely identified if no additional watermarks by unauthorized persons have been encoded into the SD.

II.c) Individual copyright, content, and originality protection

As shown in Fig. 1, the apparatus for the individual copyright , content, and originality protection is partitioned into two processes, namely the CH with the distinguished name H and the B process with the distinguished name B. Suppose (ps_H,vs_H) and (pc_H, vc_H) are asymmetric key pairs of H, (ps_B,vs_B) and (pc_B, vc_B) are the asymmetric key pairs of B. Suppose H has an authentic copy of vs_B, vc_B and B has an authentic copy of vs_H, vc_H. Then the same phases as for II.b) have to be applied.

Remark:

In the case of a legal copyright dispute, H can retrieve the payload of the detection watermark and construct the signature taken as the seed for the private watermark. Since the generation of the same asymmetric key pair by two distinguished entities is very unlikely, the generation of the digital signature as the seed for the private watermark provides a good level of proof against copyright infringement. In the case of watermark protection with registered keys, the generation of the same asymmetric key pair by two distinguished entities can be prevented.

III. Embedding the watermarks

The watermarking technique described here comprises the following steps:

a) An error-control coding technique for the message to be transmitted in the watermark;

b) A method to encode respectively to decode the message resulting from step a);

c) A reliable method for embedding the encoded message from step b) in the image or video without introducing visible artifacts.

d) A watermark extraction technique that is robust against compression, translation, rotation, scaling or change of proportion of the stego image or video.

e) A watermarking technique for small and or irregular blocks.

f) A method that allows to detect if a stego-image was marked or not with a given key without extracting the encoded message.

g) A method for watermarking without template which is resistant to translation, rotation and scaling.

h) A method for watermarking videos.

Each of these aspects can be applied to conventional watermarking techniques. Preferably, they are used in combination to provide a highly reliable, robust and powerful method for marking data sets. This method can be applied for any watermarking applications, in particular to the application described in section II of this disclosure.

Steps a) and b) can be used for embedding watermarks in any type of data while steps c) is optimized for embedding watermarks in images or video frames.

In the following, the above mentioned elements of the watermarking technique are described in detail.

III.a) Error control coding

Error control coding is applied to the message prior to encoding step III.b). When used in combination with the procedure described in section II, the message corresponds to one of the blocks BL_i.

Preferably, symbol based Reed Solomon (RS) codes are applied for this purpose. The advantages are the following:

- RS codes correct symbol errors rather than bit errors, and

- RS codes can correct erasures as well as errors. Erasures can be factored out of the key equation, which means that "erased" symbols can be ignored. They do not play any role in the error control mechanism - an erasure is useless redundancy.

Being able to discard erased symbols has two advantages:

- If the posterior probability of a received symbol is low, it may be ignored.

- RS codes only come in standard sizes. For example a 255 x 8 bit code is common. Most commonly used RS error control codes appear to be too large to be used in watermarking. However, it is possible to make almost any RS code fit a watermarking application by judiciously selecting symbols as being erased (because they were never embedded in the image in the first place).

III.b) Encoding the message

During encoding, the message to be transmitted in the watermark is transformed into a form suited for being used in the modulation of image components. At the same time, it is encrypted using a suitable key.

If used with the method of section II, the encoding procedure has access to the cryptographic keys p_H and v_H (or their hash values), which are applied as seeds to generate pseudo-random sequences as described below. The public key is used for encoding the message of the public watermark, the private key is used for the private watermark. Knowledge of the corresponding key (or hash value) is required for recovering the message from the watermark.

A watermark may be embedded or extracted by the key owner. In this form spread spectrum is a symmetric key cryptosystem. From the point of view of embedding watermarks in images or videos given the cryptographic keys the sequences themselves can be generated. A good

spread spectrum sequence is one which combines desirable statistical properties such as uniformly low cross correlation with cryptographic security.

Suppose we are given a message B (e.g. that was provided with error coding in above step III.a). The message has the binary form $b_1b_2...b_L$, where b_i are its bits. This can be written in the form of a set of symbols $s_1s_2 \ldots s_M$ - most generally by a change in a number base from 2 to B. The next stage is to encode each symbol s_i in the form of a pseudo random vector of length N, wherein each element of this vector either takes the value 0 or 1. N is e.g. in the order of 1000 to 20000 (in the order of 10%-50% of the total number of image coefficients (Fourier components) that can, theoretically, be modulated).

In a preferred embodiment, this is carried out by using a pseudo random generator seeded by the key $crh(p_H)$ or $crh(v_H)$.

To encode the first symbol a pseudo random sequence v of length N + B - 1 is generated. To encode a symbol of values where $0 < s < B$ the elements v_s, v_{s+1} ... v_{s+N-1} are extracted as a vector $\mathbf{r}_1$ of length N. For the next symbol another independent pseudo random sequence is generated and the symbol encoded as a random vector $\mathbf{r}_2$. Each successive symbol is encoded in the same way. Note that even if the same symbol occurs in different positions in the sequence, no collision is possible because the random sequences used to encode them are different - in fact they are statistically independent. Finally the entire sequence of symbols is encoded as the summation:

$$\mathbf{m} = \Sigma_{i=1..M} \mathbf{r}_i$$

The pseudo-random vector $\mathbf{m}$ has N elements, each varying between 0 and M. In a next step, the elements of $\mathbf{m}$ are offset to make their mean zero. These elements will determine the strength of modulation of the Fourier components of the image in step III.c.

When decoding the watermark, a vector **m'** (read-out message) is derived from the stego-image. In oblivious watermarking, **m'** corresponds to the modulated Fourier coefficients. Hence, in general **m'** will not be equal but "similar" to **m**.

To decode s from **m'**, the elements of **m'** are first offset to make their mean zero. Then, starting from the (known) seed, the first random sequence v of length N + B - 1 is generated and the correlation of v with **m'** is calculated. The peak of the correlation indicates the offset s_1 in the random sequence that was used for generating $\mathbf{r}_1$. Then, the next random sequence v is generated and cross-correlated with **m'** to retrieve s_2, etc.

Reliable communications of the apparatus are best accommodated by using m-sequences or Gold Codes to generate the random sequences $\mathbf{r}_i$ and use amplitude modulation:

$$\mathbf{m} = \Sigma_{i=1..M} \mathbf{b}_i^* \mathbf{r}_i^*$$

where $\mathbf{b}_i^*$ and $\mathbf{r}_i^*$ are $\mathbf{b}_i$ and $\mathbf{r}_i$ in which each bit 0 was replaced by 1 and each bit 1 by -1 due to the isomorphism between the group (exclusive OR,{0,1}) and (*,{1,-1}). In this case the values of **m** are between -M and M. Then the decoding is carried out by simply cross correlating with each of the random sequences $\mathbf{r}_i$ in turn. If the correlation is negative then a binary one has been sent, otherwise a binary 0.

Gold codes and m-sequences, both insure a good reliability and security of the embedded mark. However, Gold codes have the advantage that for a given register length k ($N=2^k-1$) there is a larger choice for the key ($2^{2k}-1$ instead of 2^k-1) and a better correlation properties if only part of the sequence is used.
If M is sufficiently large, the statistical distribution of the message **m** should approach a Gaussian (Central Limit Theorem). A Gaussian distributed watermark has the advantage that it is more difficult to detect. The vari-

ance increases with order $M^{1/2}$; in other words, the expected peak excursion of the sequence is only order $M^{1/2}$.

III.c) Embedding the message in the image or video

In this step, the encoded message **m** (e.g. as obtained in the previous step) is applied to the image or a video for generating the watermark.

In contrast to steps III.a) and III.b), embedding the message in the image requires some knowledge of the nature of the data stored in the image. In the following, the image is assumed to be a two-dimensional image that can be a still image or a video frame. The method is optimized for robustness against operations generally applied to images or video frames such as translation, cropping, rotating, scaling, change of proportion. (The method is not optimized for other types of data, such as sound or text.)

In order to achieve robustness against circular translation, the image block is first subjected to a Fourier transform. Then, message **m** is used to modulate the Fourier components. In addition to this, a template is embedded in the image, which template can be used for detecting rotation, scaling or change of proportion of the image when reading the watermark. A tiling mechanism and suitable phase-dependent correction are applied for providing robustness against cropping.

Figure 4 shows a detailed diagram describing the embedding of the watermark. Calculation starts from the cover image:

1. If the image is a color image, then compute the luminance component (by replacing each pixel by g/2 + r/3 + b/6, where g, r and b are its green, red and blue components) and use these values for the following calculations.
2. If a predefined block size (N_b)is used, divide the image into adjacent blocks of size N_b x N_b (e.g. 128 x

128 pixels). Otherwise N_b is the minimum of the image height and width (N_b =min(height, width)).

3. Map the image luminance levels (or gray levels for a black and white image) because it corresponds to a perceptually "flat" domain by replacing them with their logarithm. The logarithm is a good choice because it corresponds of the Weber-Fechner law which describes the response of the human visual system to changes of luminance.
4. Compute the FFT (Fast Fourier Transform) of each block. From the real and imaginary components obtained in this way, calculate corresponding magnitude and phase components.

   The magnitude components are translation invariant and will therefore be used in the following modulation steps. (However, it is possible to derive translation invariants from the phase spectrum as well, which could also be modulated).
5. Select the magnitude components to be modulated. To encode a message **m** of length N, a total number of N components are modulated. In non-oblivious watermarking, any components can be modulated. For oblivious watermarking, because of interference of the cover image with the watermark, the largest (highest energy) components (at about the lowest 10% of the frequencies) are avoided and components at medium frequencies (about next 30%-50%) are used; these frequencies are adjacent and are thus located in a band of frequencies. These figures are chosen because they generally give a good compromise between robustness and visibility of the watermark.

   There are several methods for selecting the components to be modulated, for example:

   a) The selection of the components to be modulated does not depend on the given image. Rather, the same components are selected for every image. The author as well as the reader of the watermark know

either the positions of the components to be selected in advance or a key which allows by means of a pseudo-random generator seeded by this key to generate the positions.

b) The largest components (inside the allowable frequency range) are used for modulation.

c) Almost all magnitude components in a given frequency band are used. The upper limit of the band is computed such that the number of frequencies inside the band be larger than and as close as possible to N.

In the methods b) and c) the order in which the components to be modulated can be provided by a pseudo-random generator seeded by a key known by both, author and reader.

When selecting the components to be modulated, care must be taken to preserve the symmetry imposed on the Fourier components $F(k_1, k_2)$ by the fact that the image block is real valued:

$$F(k_1, k_2) = F^*(N_b - k_1, N_b - k_2)$$

Once the magnitude components $(M_1, \ldots M_N)$ to be modulated are chosen, the corresponding value m_i of message **m** is added to or subtracted from the corresponding selected magnitude component M_i. Addition is used, if the corresponding phase component P_i is between 0 and π, subtraction if it is between π and 2π. This provides robustness against translation and cropping (see below).

Before adding/subtracting the values m_i to/from M_i, the vector **m** can be scaled to adjust the magnitude of its elements to those of the components M_i.

Generally, the elements m_i should be of the same order of magnitude as the components M_i. The depth of modulation or amplitude of the embedded signal should depend on the objective measure of the perceptual significance. The lower the perceptual significance, the higher should be the amplitude of the watermark.

Moreover, to insure a good invisibility one can use local energy and masking criterion (see J.F. Delaigle, C. De Vleeschouwer, B. Macq, "Digital watermarking", Proceedings of the SPIE Electronic Imaging: Science and Technology, vol. 2659: Optical Security and counterfeit Deterrence Techniques, San Jose, February 1996) to determine the depth of modulation. However, for simplicity, the amplitude for all components is kept constant. This constant can be predefined by the owner or can be some function of the mean and/or the variance of the energy in the image or its Fourier transform and the values of the pseudo-random vector **m** containing the encoded message (e.g. (mean(energy) + a * variance(energy))/mean(**m**), where a is a predefined constant).

6. Add a template by a second modulation of the magnitude components. This is described in more detail below.
7. Compute the inverse FFT using the phase components and the modulated magnitude components.
8. Compute the inverse of the perceptual mapping function of step 3. For Weber-Fechner law mapping, the inverse function is an exponential.
9. Replace each watermarked block in the image to obtain the stego-image.
10. If the image is a color image, then rescale the red, green and blue components by the relative change in luminance introduced by embedding a watermark. Typically, the red, green and blue pixels occupy a byte each in program memory. If overflow or underflow occurs then the pixel is set to the upper bound 255 or lower bound 0 respectively.

Template:

As mentioned above, a template is added to the image in step 6. Two kinds of templates can be used:

a) a RST template - to detect rotations and scaling

b) a PST template - to detect horizontal and vertical scaling.

The PST template is rather used in case of video frames (changes of proportion are more likely to occur in the case of videos than rotations) and the RST is rather used for still images (photographs, paintings, etc,...).
The steps for generating the template are illustrated in Fig. 5:

20. Apply a log-polar or a log-log map to the magnitude components. The log-polar map transforms the magnitude components of the FFT into a polar coordinate system (Θ, log-r) with logarithmic radius axis as follows. Consider a point $(x,y)\in\Re^2$ and define:

$$x = e^{\mu}\cos\Theta$$
$$y = e^{\mu}\sin\Theta$$

where $\mu\in\Re$ and $0 \le \Theta < 2\pi$. If $r = e^{\mu}$, $\mu = \log(r)$ and for every point(x,y) there is a unique $(\Theta,\log(r))$ that corresponds to it. In the log-polar representation, a scaling of the image leads to an offset of the components along the log-r axis and a rotation of the image leads to an offset along the Θ axis. Similarly, the log-log map transforms the magnitude components into a logarithmic coordinate system (log-x, log-y) as follows. For each point $(x,y)\in\Re^2$ define:

$$x = e^{\alpha}$$
$$y = e^{\beta}$$

Then, $\alpha=\log(x)$ and $\beta=\log(y)$, and in this log-log representation, the horizontal respectively vertical scaling leads to offsets along the log-x respectively log-y axes.

21. Preferably, low pass filtering is used for interpolating the frequency space components during this mapping. The magnitude components belonging to very low or high frequencies are not mapped. The following modulation is only applied to components in medium frequency range.

22. Select the magnitude components in the log-polar or log-log coordinate system to be modulated. Typically, about 0.1-0.3% of all components are to be modulated. The RST or PST pattern **T** formed by the selected components in log-polar or log-log space should be such that its auto-correlation under translation is weak. For this purpose, the indices of the selected components should be coprime or be derived from a two-dimensional random sequence. This random sequence can be generated by a random generator seeded by a key K. Whoever knows this key K will be able to reconstruct the template and detect the watermark as explained below. Each selected component is increased by a given value.
23. Map the modulated points by change of coordinates back into frequency space(inverse log-polar mapping or inverse log-log mapping).

The RST or PST pattern **T** formed by the selected components in log-polar respectively log-log space is predefined and known to the reader of the watermark.
It must be noted that the calculation of the log-polar respectively log-log transform of the cover image or video frame is not required for generating the template. Instead, the RST or PST pattern **T** of the components to be modulated in log-polar respectively log-log space can be mapped back to frequency space, which results in a RST or PST pattern **T'** in frequency space that can be applied directly to (e.g. added to) the components in frequency space. Alternatively, the template can be added directly in the Fourier transform domain.
As will be explained below, the template is not required for non-oblivious watermarking.

III.d) Extracting the watermark from the stego-image or video

Figure 6 shows a detailed diagram illustrating the steps for reading a watermark from the stego-image or stego video frame:

31. If the image is a color image then compute the luminance component and use these values for the following calculations.
32. If predefined block size (N_b) is used, divide the image into adjacent blocks of size N_b x N_b (e.g. 128 x 128 pixels). Otherwise N_b = min(height, width).
33. Map the image luminance levels (or gray levels) to the perceptually "flat" domain by replacing them with their logarithm.
34. For each block compute the FFT.
35. Use a data windowing process to suppress the edge effects in the magnitude spectrum due to possible rotation or scaling of the image. Different windows can be used such as Blackman, Hamming, Hanning, Welch or Bartlett Window (see W.H. Press, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery, "Numerical Recipes in C", Cambridge University Press, second edition, 1992). The effect of data windowing in the space domain is equivalent to convolution in the frequency domain with a narrow filter. The blurring effect introduced by this convolution is beneficial because it tends to smooth the spectrum which makes interpolation more effective.
36. Determine the rotation and scaling that the image suffered by finding the RST template in log-polar space or determine the horizontal and vertical scaling by finding the PST template in the log-log space. These steps are described below in "Finding the template" section.
37. Using the results of step 35, read the modulated components to generate message **m'**. This requires the knowledge of the method that was used in step 5 for selecting the components to be modulated.

Once that the message **m'** is recovered, it is demodulated and error corrected using the methods described in sections III.a) and III.b).

Finding the template:

The steps for finding the template are illustrated in Fig. 7:

40. Apply log-polar or log-log mapping to the magnitude components of the Fourier transform. The magnitude components belonging to very low or high frequencies are not mapped. The following analysis is only applied to components in medium frequency range or to all components except the low frequency range.

41. For oblivious watermarking, calculate the normalized cross correlation of the components in log-polar or log-log space with the RST or PST pattern **T** that was used for generating the template in step 21 and find the point of best correlation. If the image has neither been rotated or scaled, this point is at zero. If the image is rotated and/or globally scaled there is an offset along the Θ axis and/or log-r axis, in the log-polar map. If the scaling suffered by the image or video frame was different on horizontal respectively vertical axis, there are offsets along log-x respectively log-y axes in the log-log map. For non-oblivious watermarking, the log-polar respectively log-log transform of the Fourier components of the cover image can be used instead of RST or PST pattern **T** for retrieving scaling, rotation respectively change of proportion
The cross correlation can be calculated efficiently using conventional Fourier techniques.

In order to obtain better results and lower computational cost, before applying the cross correlation one can first adaptively filter the data to remove outliers and noise and use a filter which keeps only local peaks. This can e.g. be carried out by locally calculat-

ing the variance (or some other value indicative of the data's distribution) of neighbouring data of each data point. If a given data point lies clearly outside this variance, is it replaced by zero. In a next step, local peaks that have not been filtered out are then stored in a sparse matrix to reduce computation. The fast correlation (using the FFT or by a point by point correlation) is done in this case between the peaks of (**T**) and the peaks of (**T'**). The correlation can moreover be weighted so that the more reliable central points are more strongly weighted.

It is possible to further increase accuracy of the scaling and rotation factors by carrying out the following: detecting a scaling and/or rotation in a first iteration from the correlation between the log-polar or log-log transform and the template, using said scaling and/or rotation for either a) scaling and/or or rotating said Fourier transform, calculating a scaled and/or rotated log-log or log-polar transform therefrom and correlating said rotated log-log or log-polar transform with said template, or b) calculating a second template by scaling and/or rotating an original Fourier-space template and calculating a log-log and or log-polar transform therefrom and using said second template for calculation a second correlation with said log-log or log-polar transform of said stego data

III.e) Embedding watermarks in small and/or irregular blocks

To embed watermark in small blocks, one computes the transform over regions that instead of comprising only one block, extend over adjacent blocks. To do this one can use the Lapped Orthogonal Transform (see H.S. Malvar, "Signal Processing with Lapped Transforms", Norwood, MA, 1991) which has the advantage to minimize blocking effects which would otherwise make a strong watermark based

on blocks visible, especially for small block sizes. This is followed by the method as described in III.c and III.d, where the Fourier transformation phase is replaced by the Lapped Orthogonal Transform (LOT) application for the cover image, while keeping the same template operations.

Using small blocks (of roughly 16 by 16 points) allows the strength of the embedded message to be modulated as a function of the local variance, which renders the method adaptive. Furthermore the watermark can be recovered locally the only requirement being that a sufficient number of blocks are available to contain 1 complete message.

To embed watermark in blocks with irregular shapes (non-square and non-rectangular) such as might occur in MPEG4 video compression, two possible solutions can be applied:

- padding of the irregular blocks in order to obtain square blocks, using either constant padding, or symmetrical padding, then method as in III.c and III.d;
- avoid the padding phase by directly using wavelet transforms of arbitrary length signals (see H.S. Barnard, Image and Video Coding Using wavelet decomposition, CIP-Gegevens, Koninklijke Bibliotheek, Den Haag, 1994). This is followed by the method as described in III.c and III.d, where the Fourier transformation phase is replaced by the Wavelet Transformation for the cover image, while keeping the same template operations.

III.f) Watermark detection without extraction

Being able to detect a watermark without being able to decode it is useful and in many cases sufficient to prove the identity of the generator of the watermark. This can be done by a Bayesian approach (see J.J.K. Ó Ruanaidh and W.J. Fitzgerald, "Numerical Bayesian Methods Applied to Signal Processing", Series on Statistics and

Computing, Springer-Verlag, 1996) that allows to compute the probability that a watermark generated by a given key is present in the stego-image, relatively to the probability that no watermark was generated with that key.

The implementation of this principle operates as follows. The used watermark **d** is a linear combination of pseudo-random sequences corrupted by noise:

$$\mathbf{d} = \mathbf{G}\,\mathbf{b} + \mathbf{e}$$

where **e** is a noise vector corrupting the watermark, **b** is an M x 1 vector and **G** is an N x M matrix of bits in form +1 and -1 (due to the isomorphism between the group (exclusive OR, {0,1}) and (*, {1,-1}) 0 was changed to 1 and 1 to -1). Each column of **G** is a pseudo-random sequence such as an m-sequences or a Gold Code in which 0 was changed to 1 and 1 to -1.

If we assume that the noise follows a Gaussian distribution, the probability that a message of length M was embedded with a said key k in the stego-image (SD) is:

$$p(k,\mathrm{M}\,|\,\mathbf{d},SI) \propto \frac{\pi^{-\mathrm{N}/2}\Gamma(\mathrm{M}/2)\Gamma((\mathrm{N}-\mathrm{M})/2)\det(\mathbf{G}^{\mathrm{T}}\mathbf{G})^{-1/2}}{4R_{\delta}R_{\sigma}(\hat{\mathbf{b}}^{\mathrm{T}}\hat{\mathbf{b}})^{\mathrm{M}/2}(\mathbf{d}^{\mathrm{T}}\mathbf{d}-\mathbf{f}^{\mathrm{T}}\mathbf{f})^{(\mathrm{N}-\mathrm{M})/2}}$$

where Γ is the gamma function, R_{δ} and R_{σ} are irrelevant constants introduced as normalization factors,

$$\hat{\mathbf{b}} = (\mathbf{G}^{\mathrm{T}}\mathbf{G})^{-1}\mathbf{G}^{\mathrm{T}}\mathbf{d}$$

and

$$\mathbf{f} = \mathbf{G}^{\mathrm{T}}\hat{\mathbf{b}}$$

The probability that no message was embedded with the said key k in the stego-image (SD) is:

$$p(k,0\,|\,\mathbf{d},SI) \propto \frac{\pi^{-\mathrm{N}/2}\Gamma(\mathrm{N}/2)}{2R_{\sigma}\,(\mathbf{d}^{\mathrm{T}}\mathbf{d})^{\mathrm{N}/2}}$$

Finally, we compute the relative log-probability:

$$\log\left(\frac{p(k,\mathrm{M}\mid\mathbf{d},SI)}{p(k,0\mid\mathbf{d},SI)}\right)$$

and compare with 0.

III.g) Watermarking without template

Using a combination of Fourier transform and a log-polar map, i.e. the Fourier-Mellin transform that is the Fourier transform of a log-polar map, allows to embed a watermark in a domain that is invariant to rotation, scale and translation, without the need to use a template to detect rotations and scaling. The method consists of directly transforming the cover-image or -video frame in the log-polar domain; the watermark is directly inserted at this stage. Figure 8. shows the steps for embedding the watermark in a rotation, scale and translation invariant domain.

An alternative which is computationally more efficient bypasses the mapping of the original image or video frame in the rotation, scale and translation invariant domain. This is shown in Figure 9. The scheme to extract the watermark from the image is shown in Figure 10.

Replacing the log-polar mapping by the log-log mapping allows to embed a watermark in a domain that is invariant to translation, horizontal and vertical scaling.

This is an idealized watermarking scheme which works in principle but which in practice is quite costly and difficult to implement. The first difficulty is that both the log-polar mapping (LPM) and the inverse log-polar mapping (ILPM) can cause a loss of image quality. The change of coordinate system means that some form of interpolation must be used. This leads to a second difficulty, which is rather numerical. Interpolation only performs well if the neighboring samples are of the same

scale, which is not verified by the magnitudes of the frequency components.

III.h) Watermarking videos

In the case of uncompressed video each frame is marked. One possibility is to use the same key and the same watermark in each frame. However this can decrease the robustness of the watermark against forgery. Therefore, it is preferable to use the same key, but a different watermark for each frame (e.g. the label of the video followed by the frame number). In the case of MPEG1 or MPEG2 compressed video, only the intraframes I (the first frame of each group of pictures) are marked.

Another novel alternative for watermarking uncompressed video is to individually mark three-dimensional spatio temporal blocks of video stream, which may be overlapped in time and/or in space. The method used here is an extension of the algorithms used for 2D images to the temporal dimension, using 3D Fourier transform, 3D template, and the same spread spectrum techniques to generate the watermark. The use of Fourier transform ensures the same rotation, scaling, and proportion invariances. We have also a full invariant 3D watermark for theses blocks, exactly as for 2D still image watermarking. These 3D blocks may be rather large, or small enough to ensure more robustness against cropping. As for individual frame marking, we can use the same watermark for all blocks, or a different watermark for each block. The advantage of this spatio temporal approach is to take in account the motion and scene variation in watermarking, as developped in the paper of M.D. Swanson, B. Zhu and A.H. Tewfik, "Multiresolution Scene-Based Video Watermarking using Perceptual Models", IEEE Journal on Selected Areas in Communications, vol. 16, no. 4, May 1998. However, in contrast with our apparatus,

they make use of 1D temporal wavelets transform instead of our 3D Fourier transform.

IV. Properties of the watermark:

In the following, some of the properties of the watermark generated using the steps described above are discussed.

Resistance to cropping:

One feature of translation invariants developed using the Fourier transform is that they are invariant to circular translations (or cyclic shifts). This is used to construct watermarks that are invariant to cropping. This is illustrated by reference to Figs. 11 and 12.

As mentioned above, the image is split into blocks and the watermark is applied to each block. In other words, the same modulation pattern is applied to the Fourier components of each block, wherein the modulation pattern is given by the corresponding encoded messages **m**.

Fig. 11 shows such an image where the fat lines 100 designate the borders between the blocks. Suppose that the watermark in a standard size block will be of the form:

T=[A B ; C D]

where the sub-matrices A, B, C and D are of arbitrary size. A circular translation of such a watermark is of the form:

S=[D C ; B A].

The original stego-image is tiled with watermarks in the pattern [T T T T ; T T T T ;T T T T]. Therefore, a cropped section of the matrix will carry a watermark in the form [S S S S ; S S S S ; S S S S]. This is illustrated in Figure 12. When reading the watermark of

the cropped image of Fig. 12, each block carries the watermark S. Since S is a circular transform of T, it can be read without problems in the Fourier domain using the steps outlined above.

Note, however, that the cover image is not tiled, only the watermark is. Therefore, while cropping merely induces a circular translation of the watermark in each block, the change of image in each block is not a circular translation. To compensate for this, the phase components P_i of the Fourier transform must be used for correcting the sign of the modulation of the magnitude components M_i, as it is outlined under step 5 above.

The optimum size of block depends on a number of different factors. A size that is a power of two is useful because the FFT can be used. The block size also must be small enough to withstand cropping but large enough to comfortably contain a watermark. The best compromise for block size is 128.

Resistance to scaling and rotation:

As mentioned above, reading the RST template in log-polar space allows to detect and measure any scaling and/or rotation that was applied to the image. This information can then be used for reading the watermark. Since the reader knows the pattern that was used for modulating the magnitude components in step 5, he can identify the modulated components in the scaled and rotated image and derive the message **m'** therefrom. An alternative is to compensate the transformation using the measured rotation and scaling and read the message in the compensated image.

Note that the apparatus does not explicitly use a rotation and scale invariant watermark but instead searches the parameter space of rotations and scales. Since searching the space of rotation and scales in the frequency or space domain is quite complicated (as e.g. described in the WO 96/36163), the log-polar map is used

where these parameters are Cartesian coordinates and can be searched using efficient correlation techniques.

Resistance to change in aspect ratio:

Similarly as above, reading the PST template in log-log space allows to detect and measure the horizontal and vertical scaling that was applied to the image or video frame. This information can then be used to compensate the transformation, which the allows the watermark to be read.

The use of the log-polar map (LPM) or log-log map (LLM) changes depending on whether the watermark was inserted block by block of predefined size in the FFT domain or whether the block size depends on the image size. In the first case, the LPM or LLM is used to detect scale changes in the image. In the latter case, the maps are used to detect the ratio between the FFT size used in embedding (which is unknown since the original image size is unknown in oblivious watermarking) and the FFT size used in extraction, which equals the size of the image in which we attempt to extract the watermark. This is important in cases where the image size has changed as a result of e.g. cropping or rotation since the relative positions of the FFT points change.

Lossy compression:

The robustness of the watermark to operations such as lossy compression is achieved by using a perceptually adaptive spread spectrum communications approach, in which a spread spectrum signal is embedded in selected components of the magnitude spectrum of the Fourier Transform of the image.

Redundancy:

The watermark is embedded in blocks of a fixed size with exactly the same watermark embedded in each block. This means that the watermark can be recov-

ered from a single block only. This leads to a redundancy that increases the chance of extracting the watermark correctly from more than one block.

V. Summary

The following summarizes some of the properties of the preferred embodiments of the invention.

The use of an asymmetric cryptographic key pair for the seed generation enables the execution of asymmetric key agreement protocols with message recovery or appendix and the protection of the communication between the involved parties. Different security services for the communication, such as mutual authentication, integrity, confidentiality and non-repudiation are supported by the system with one asymmetric cryptographic key pair of the watermark author only for a registration or trading process

The present technique enables a strong binding relation between the image ID, the image, and the CH if the CH registers his copyright at the CCC. If an image is watermarked later by an unauthorized person, the time stamp in the copyright certificates resolves the copyright ownership.

The CH does not have to reveal his private cryptographic key if ownership verification has to be applied by a different legal party.

The present technique supports transferal of copyrights. If copyright is transferred to another legal party, corresponding copyright revocation certificates may be generated.

Digital signatures techniques are applied for the security of the communication between different parties and the authentication data embedded in a private or public watermark of an image or video. No signature labeling techniques of the complete image or video are applied by the system.

In addition, originality protection and image content protection by ciphering/deciphering in the transform domain is supported.

The Fourier Mellin transform is the Fourier Transform of a log-polar map. It allows to embed a watermark in a domain that is invariant to rotation, scale and translation. However this approach is costly and difficult to implement, and therefore it has been enhanced by combining with a Fourier Transform based template embedding technique.

In the present invention, the log-polar map of a Fourier transform is used as a means of facilitating rotation and scaling invariance. In order to be invariant to scaling and change of proportion, the log-log map of the Fourier transform is also used.

Circular translation invariants are used as a means of constructing digital watermarks that are invariant to cropping.

In contrast to some known techniques, the present system does not require a database of all watermarks that were ever embedded in image anywhere.

Information is embedded and/or retrieved in the log-polar or log-log domain of the Fourier transform. Frequency components are modulated which are oblivious to the cover image but which also have the property that they form an unambiguous non-repeated pattern in log-polar respectively log-log space. They are used for determining the degree of rotation and scaling respectively the change of proportion suffered by a stego-image in the absence of the cover-image. Coprime frequencies are useful for generating such a pattern or template. Uniform random sampling of log-polar or log-log space is another method that can be applied.

The technique applies a new concept of invariants which eliminate the need for explicitly searching for rotation and/or scaling values.

The methods described above can be incorporated into an apparatus, such as one or more computers, using know programming and hardware techniques. To prove the feasibility of the approach, a Java based copyright protection and authentication environment for digital images has been implemented. The PKI, the CH, the CCC, and the IB application processes all implement a Graphical User Interface and a server, supporting both console users and other requests through a socket interface.

While there are shown and described presently preferred embodiments of the invention, it is to be distinctly understood that the invention is not limited thereto but may be otherwise variously embodied and practiced within the scope of the following claims.